State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

January 13, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-004

DATE ISSUED:
01/12/2016

SUBJECT:
Cumulative Security Update for Internet Explorer (MS16-001)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer. These vulnerabilities could allow an attacker to execute code in the context of the browser if a user views a specially crafted web page. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Depending on the privileges associated with the user, an attacker may install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Microsoft Internet Explorer is prone to multiple vulnerabilities that could allow remote code execution. The vulnerabilities are as follows:

- A Scripting Engine Memory Corruption Vulnerability exists that could allow for remote code execution (CVE-2016-0002)
- An Elevation of Privilege Vulnerability exists that could allow for an attacker to bypass security restrictions (CVE-2016-005)

The most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. When the website is visited, the attacker's script will run within the context of the affected browser or with the same permissions as the affected user account. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The elevation of privilege vulnerability by itself does not allow arbitrary code to be run. However, the vulnerability could be used in conjunction with another vulnerability, such as a remote code execution vulnerability, that could take advantage of the elevated privileges when running arbitrary code. For example, an attacker could exploit another vulnerability to run arbitrary code through Internet Explorer, but due to the context in which processes are launched by Internet Explorer, the code might be restricted to run at a low integrity level (very limited permissions). However, an attacker could, in turn, exploit this vulnerability to cause the arbitrary code to run at a medium integrity level (permissions of the current user).

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- A work around for CVE-2016-0002 is to restrict access to VBScript.dll. The command line instructions to accomplish this are available in Microsoft Security Bulletin MS16-001.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS16-001

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0002
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0005